Explore

golang

Implement a threshold decryption Service.

??

Possible to perform parallely -

Explore-go

A common package using golang that provides essential utilities.

Read necessary information to understand

Threshold Cryptography

Consider

construction of robust and secure threshold Schemes.

Action Items:

1. Github repository for "explore-go" repo
2. Research carefully to come up with possible best solution for this specific problem domain.

Note -2

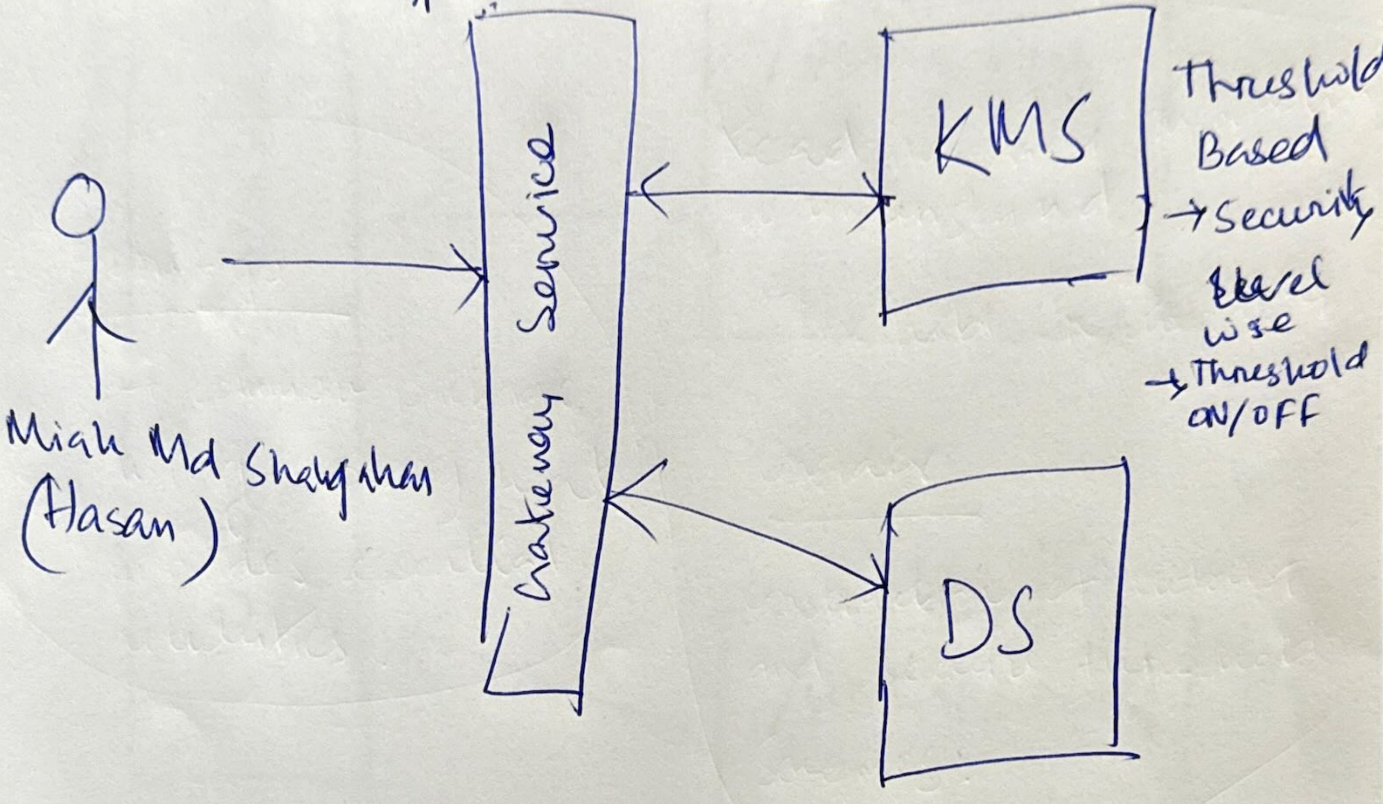
might be fit

✓ Pair based Cryptography

✓ Shamir's Secret Sharing

Distributed system

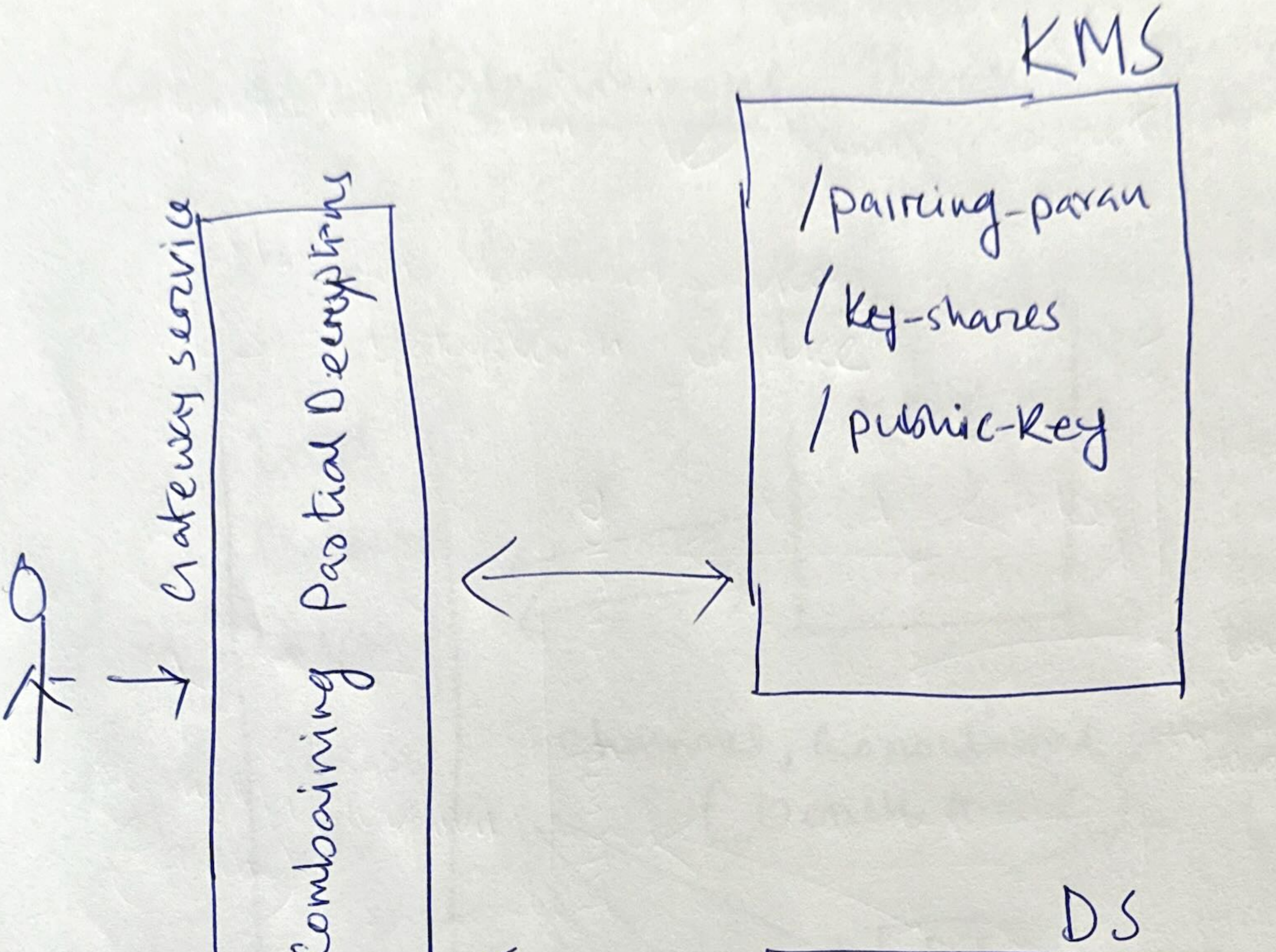
KMS = Key Management Service
DS = Decryption Service



Questions

1. What types of Gateway Service do we need? (Gateway as a Proxy / Gateway as orchestration)

Note - 3

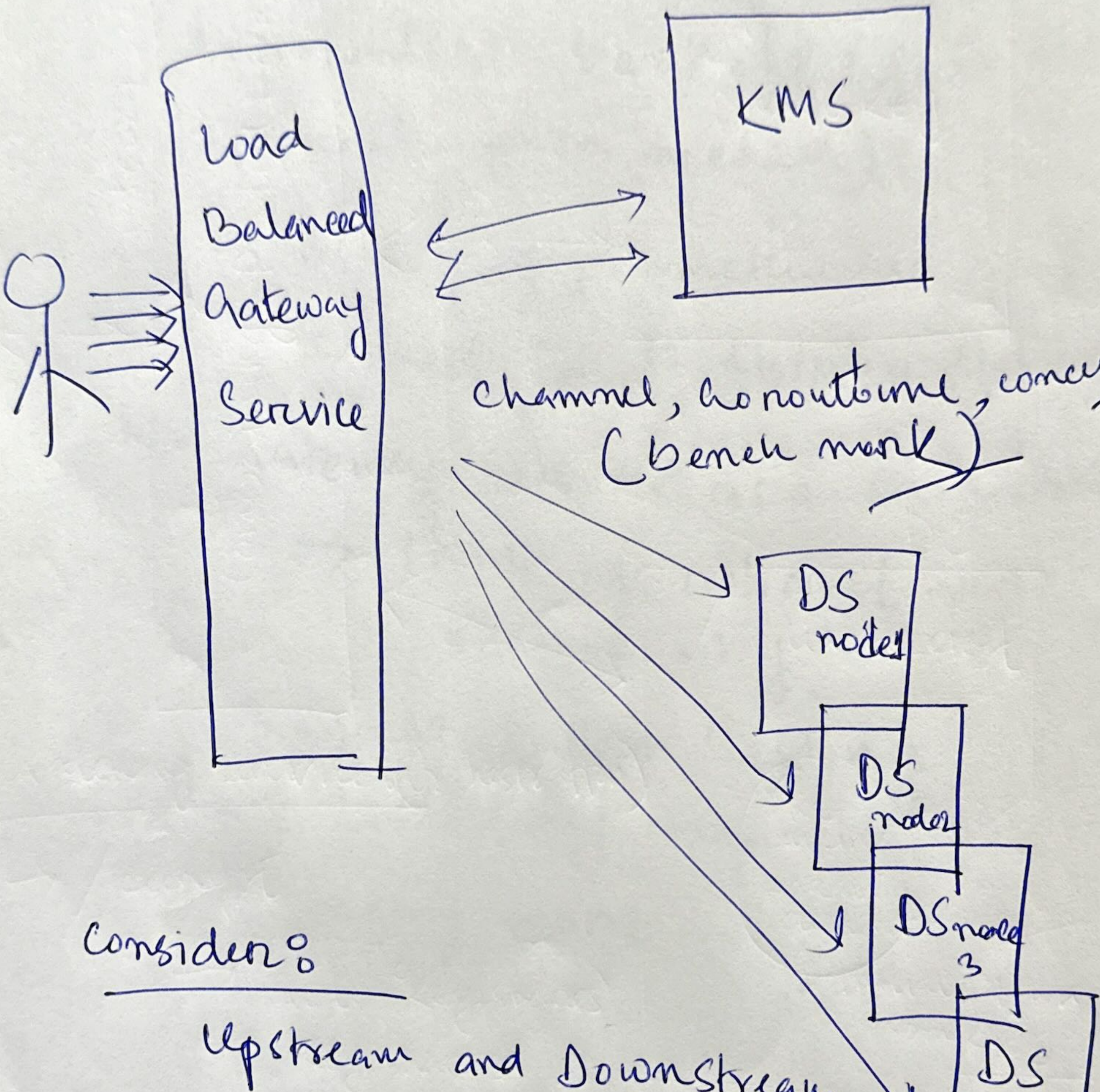


Gateway Services (Orchestration)

- ↳ /decrypt
  - ↳ Get "key-shares" /key-shares during initialization from KMS
  - ↳ Go to DS service with client provide ciphertext and KMS retrieved "key-shares"
  - ↳ combine results.

Note-1

Consider Asynchronous threshold Decryption:



Consider:

Upstream and Downstream resiliency of distributed system

→ Retry, Rate limit, Retry amplification

Note-4.1

- Service to Service health check
- Retry with considering amplification, exponential backoff (fail fast approach when needed).
- Monitory → promethuous, grafana, Request Id to distruibuted logging.
- Gateway service as a Orchestration
  - → Think of robougt and scalebe way.
  - → Mutation Testing
- Rate limilting ⇒
- many more ....

=